

UNITED STATES DISTRICT COURT

for the
Eastern District of Wisconsin

In the Matter of the Search of)
(Briefly describe the property to be searched)
or identify the person by name and address))
information associated with NIAZ1642711@GMAIL.COM,)
HOLDPARKCY@GMAIL.COM, AND)
MAHSA.ALIZADEH.83@GMAIL.COM, (See Attachment A))

Case No.22-981M(NJ)

Matter No.: 2019R00440**WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS**

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search and seizure of the following person or property located in the _____ District of _____

(identify the person or describe the property to be searched and give its location):

See Attachment A; over which the Court has jurisdiction pursuant to 18 U.S.C. §§ 2703 and 2711 and Federal Rule of Criminal Procedure 41.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal (identify the person or describe the property to be seized):

See Attachment B.

YOU ARE COMMANDED to execute this warrant on or before September 8,2022 (not to exceed 14 days)

☒ in the daytime 6:00 a.m. to 10:00 p.m. ☐ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to _____

Hon. Nancy Joseph

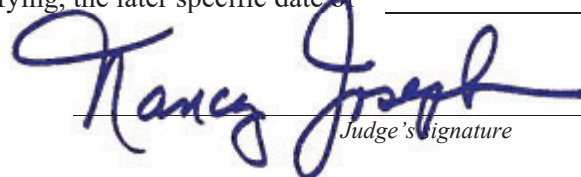
(United States Magistrate Judge)

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized (check the appropriate box)

☐ for _____ days (not to exceed 30) ☐ until, the facts justifying, the later specific date of _____

Date and time issued:8/25/2022 @ 2:09 p.m.

City and state: Milwaukee, WI



Judge's signature

Hon. Nancy Joseph, U.S. Magistrate Judge

Printed name and title

Return		
Case No.:	Date and time warrant executed:	Copy of warrant and inventory left with:
Inventory made in the presence of :		
Inventory of the property taken and name(s) of any person(s) seized:		
Certification		
<p>I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.</p> <div style="display: flex; justify-content: space-between; align-items: flex-end;"> <div style="width: 30%;"> <p>Date: _____</p> </div> <div style="width: 65%;"> <p style="text-align: center;">_____</p> <p style="text-align: center;"><i>Executing officer's signature</i></p> <p style="text-align: center;">_____</p> <p style="text-align: center;"><i>Printed name and title</i></p> </div> </div>		

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with NIAZ1642711@GMAIL.COM, HOLDPARKCY@GMAIL.COM, AND MAHSA.ALIZADEH.83@GMAIL.COM that is stored at premises owned, maintained, controlled, or operated by Google LLC, a company headquartered at Mountain View, CA.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Google LLC (the “Provider”)

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, regardless of whether such information is located within or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to the Provider, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f) on February 7, 2020 the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A:

a. The contents of all emails associated with the accounts from **June 1, 2014 to the present** including stored or preserved copies of emails sent to and from the accounts, draft emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email;

b. All records or other information regarding the identification of the accounts, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

c. The types of service utilized;

d. All records or other information stored by an individual using the accounts, including address books, contact and buddy lists, calendar data, pictures, and files; and

e. All records pertaining to communications between the Provider and any person(s) regarding the accounts, including contacts with support services and records of actions taken.

The Provider is hereby ordered to disclose the above information to the government **14 DAYS** of issuance of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, contraband, evidence, and instrumentalities of violations of 50 U.S.C. § 4819, and 50 U.S.C. § 1705, those violations involving Bahador Akbarnia, and others and occurring after **June 1, 2014**, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

- (a) Evidence of violations of the U.S. Export Control Reform Act and/or the International Emergency Powers Act;
- (b) Evidence of violations of Iranian Transactions and Sanctions Regulations;
- (c) Evidence of a conspiracy to ship items from the United States to Iran via the UAE in violation of U.S. sanctions against Iran;
- (d) Evidence indicating how and when the email accounts were accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the email accounts owners;
- (e) Evidence indicating the email accounts owners' state of mind as it relates to the crime under investigation;
- (f) The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s).
- (g) The identity of the person(s) who communicated with the user ID about matters relating to the illegal export of items to Iran, including records that help reveal their whereabouts.

UNITED STATES DISTRICT COURT

for the
Eastern District of Wisconsin

In the Matter of the Search of

*(Briefly describe the property to be searched
or identify the person by name and address)*information associated with NIAZ1642711@GMAIL.COM,
HOLDPARKCY@GMAIL.COM, AND
MAHSA.ALIZADEH.83@GMAIL.COM, (See Attachment A)

Case No. 22-981M(N)

Matter No.: 2019R00440**APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS**

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

See Attachment A; over which the Court has jurisdiction pursuant to 18 U.S.C. §§ 2703 and 2711 and Federal Rule of Criminal Procedure 41.

located in the _____ District of _____, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:


- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

<i>Code Section</i>	<i>Offense Description</i>
Title 50 U.S.C. § 4819	The Export Control Reform Act ("ECRA")
Title 50 U.S.C. § 1705	The International Emergency Powers Act ("IEEPA")

The application is based on these facts:
See attached affidavit.

- ☒ Continued on the attached sheet.
- ☐ Delayed notice of _____ days *(give exact ending date if more than 30 days)* _____ is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

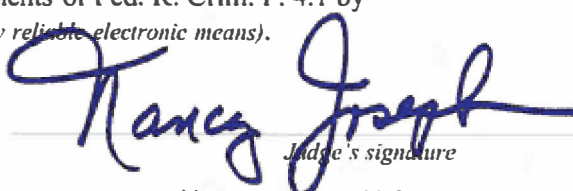

*Applicant's signature*SA Jon Svendsen, BIS
Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by
telephone _____ *(specify reliable electronic means)*.

Date: 8/25/2022

Milwaukee, WI

City and state: _____


Judge's signature

Hon. Nancy Joseph, U.S. Magistrate Judge

Printed name and title

**AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT**

I, Jon Svendsen, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent with the Department of Commerce (“DOC”), Bureau of Industry and Security (“BIS”), Office of Export Enforcement (“OEE”), and have been so employed as a federal law enforcement officer since December 2003. While employed by BIS as a federal law enforcement officer, I have conducted criminal investigations concerning United States export controls and sanctions, authored affidavits and complaints, and collected evidence to be used in prosecution. I have received formal training from the Federal Law Enforcement Training Center in Glynco, Georgia, as well as specialized training related to counter proliferation investigations and United States export controls.

2. I make this affidavit in support of an application for a search warrant for information associated with certain accounts that are stored at premises controlled by Google LLC, an email provider headquartered at Cupertino, California. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Google LLC to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

3. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of ECRA, Title 50, United States Code § 4819, and IEPA, Title 50, United States Code, § 1705 have been committed by Bahador Akbarnia

(hereinafter, “AKBARNIA”), and other persons. There is also probable cause to search the information described in Attachment A for evidence, instrumentalities, contraband, and/or fruits of these crimes further described in Attachment B.

4. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

5. The statements in this affidavit are based on my personal knowledge, and on information I have received from other law enforcement personnel and from persons with knowledge regarding relevant facts.

6. The accounts to be searched are:

NIAZ1642711@GMAIL.COM

MAHSA.ALIZADEH.83@GMAIL.COM

HOLDPARKCY@GMAIL.COM

JURISDICTION

7. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is “a district court of the United States . . . that has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

APPLICABLE LAWS AND REGULATIONS

ECRA - Pub. L. No. 115-232, tit. 17, subtitle B, 132 Stat. 2208 (2018)

8. The Export Control Reform Act of 2018 ("ECRA") provides, among its stated policy objectives, that "the national security and foreign policy of the United States require that the export, reexport, and in-country transfer of items, and specific activities of United States persons, wherever located, be controlled" Pub. L. No. 115-232, § 1752, 132 Stat. 2208 (2018).

To that end, ECRA grants the President the authority "(1) to control the export, reexport, and in-country transfer of items subject to the jurisdiction of the United States, whether by United States persons or by foreign persons; and (2) the activities of United States persons, wherever located, relating to" specific categories of items and information. ECRA § 1753. ECRA further grants the Secretary of Commerce the authority to establish the applicable regulatory framework.

9. Pursuant to that authority, the Department of Commerce ("DOC") reviews and controls the export of certain items, including goods, software, and technologies, from the United States to foreign countries through the Export Administration Regulations ("EAR"), 15 CFR §§ 730-774. In particular, the EAR restricts the export of items that could make a significant contribution to the military potential of other nations or that could be detrimental to the foreign policy or national security of the United States. The EAR imposes licensing and other requirements for items subject to the EAR to be lawfully exported from the United States or lawfully re-exported from one foreign destination to another.

10. The most sensitive items subject to EAR controls are identified on the Commerce Control List, or "CCL," published at 15 CFR part 774, Supp. No. 1. Items on the CCL are categorized by Export Control Classification Number ("ECCN"), each of which has export controls requirements depending on destination, end use, and end user.

11. Pursuant to ECRA Section 1760, "[i]t shall be unlawful for a person to violate, attempt to violate, conspire to violate, or cause a violation of this part or of any regulation, order, license, or other authorization issued under this part," and pursuant to Section 1760(b), "[a] person who willfully commits, willfully attempts to commit, or willfully conspires to commit, or aids or abets in the commission of, an unlawful act described in subsection (a) shall" be guilty of a crime.

IEEPA - 50 U.S.C. § 1705

12. Enacted in 1977, IEEPA gives the President certain powers, defined in 50 U.S.C. § 1702, to deal with any threats with respect to which the President has declared a national emergency, and prescribes criminal penalties for violations. Section 1705 provides, in part, that "[i]t shall be unlawful for a person to violate, attempt to violate, conspire to violate, or cause a violation of any license, order, regulation, or prohibition issued under this title." 50 U.S.C. § 1705(a).

13. Beginning with Executive Order No. 12170, issued on November 14, 1979, the President found that "the situation in Iran constitutes an unusual and extraordinary threat to the national security, foreign policy and economy of the United States and declare[d] a national emergency to deal with that threat."

14. On March 15 and May 6, 1995, the President issued Executive Orders Nos. 12957 and 12959, prohibiting, among other things, the exportation, re-exportation, sale, or supply, directly or indirectly, to Iran of any goods, technology, or services from the United States or by a United States person, and on August 19, 1997, issued Executive Order No. 13059 clarifying the previous orders (collectively, the "Executive Orders"). The Executive Orders authorized the United States Secretary of the Treasury to promulgate rules and regulations necessary to carry out the Executive Orders. Pursuant to this authority, the Secretary of the Treasury promulgated the Iranian Transactions Regulations (renamed in 2013, the Iranian Transactions and Sanctions Regulations, the "ITSR") implementing the sanctions imposed by the Executive Orders.

15. The ITSR, Title 31, Code of Federal Regulations, Section 560.204, prohibit, among other things, the exportation, re-exportation, sale, or supply, directly or indirectly, from the United States, or by a United States Person, of goods, technology, or services to Iran or the Government of Iran (with certain limited exceptions), including the exportation, re-exportation, sale or supply

of goods, technology or services to a third country knowing that such goods, technology or services are intended for Iran or the Government of Iran, without a license from the U.S. Department of Treasury's Office of Foreign Assets Control ("OFAC").

16. The ITSR also prohibits the supply of services where the benefit of such services is otherwise received in Iran, if such services are performed in the United States. See 31 C.F.R. § 560.410. The ITSR further prohibits transactions that evade or avoid, have the purpose of evading or avoiding, cause a violation of, or attempt to violate the ITSR. 31 C.F.R. § 560.203.

Unlawful Export Information Activities – 13 U.S.C. § 305

17. Title 13, United States Code, Section 305 makes it a federal crime (1) to knowingly fail to file or knowingly submit false or misleading export information through the Shippers Export Declaration (SED) (or any successor document) or the Automated Export System (AES) or (2) to knowingly report any information on or use the SED or the AES to further any illegal activity.

PROBABLE CAUSE

Advanced Engineering Export of Thermal Cyclers to Barat FZE

18. Advanced Engineering, LLC (hereinafter, "Advanced Engineering")¹ is a business registered in Wisconsin as AE Advanced Engineering, LLC, and is located at 1833 Executive Drive, Suite 103, in Oconomowoc, WI. The business's website, aelabservices.com, indicates the business was established in 1987 and provides engineering services for fluid, process controls, and

¹ Advanced Engineering is owned and operated by Atef Alwashah, also known as Atef Arabiyat. Alwashah also owns and operates R&D Technologies LLC, which is co-located with Advanced Engineering. Historically, R&D Technologies LLC has purchased merchandise from manufacturers in the United States and Advanced Engineering exports the same merchandise to international customers.

electrical applications. Advanced Engineering frequently exports laboratory and research type merchandise to businesses located in countries within the Middle East.

19. Advanced Engineering exported fifteen thermal cyclers from the United States on or about October 4, 2019, to BARAT FZE (hereinafter, “BARAT”)², a business registered and located in the SAIF Zone, Dubai, United Arab Emirates (“UAE”). Specifically, this transaction was associated with Purchase Order 19-159, 15 thermal cyclers valued at \$37,440 USD, and air waybill 724-3026 3155.

20. An Import/Export Permit issued by the UAE government, dated October 16, 2019, provided BARAT was the consignee of lab supplies / thermal cyclers, valued at \$37,440 USD, from “Advances Engineering,” 1833 Executive Drive, Oconomowoc, WI. The permit’s end user was ARINA HAYAT DANESH PJS (hereinafter, “AHD”)³ of 2nd floor, No 14 West Tohid 5Str (address truncated), Iran. The permit further listed the invoice as 19-159, inbound air waybill as 724-30263155, and shipping route as Chicago USA – Dubai Airport – Imam Khomainsi Airport. Additionally, the permit provided email for BARAT as baratfze@gmail.com and email for AHD as mahsa.aliizadeh@gmail.com.

21. A thermal cycler (also known as a PCR machine or DNA amplifier) is a laboratory apparatus most commonly used to amplify segments of DNA via the polymerase chain reaction (“PCR”). PCR is now a common and often indispensable technique used in clinical and medical

² Publicly available information for BARAT included business license 13882, incorporation date 2014-06-09, location at SAIF Executive Office P8-03-64, and contact person listed as Shomiseh Moatazedi

³ According to <https://arinahayat.com>, AHD is located in Tehran, Iran and appears to supply equipment, installation, maintenance and service.

laboratory research for a broad variety of applications including biomedical research and criminal forensics.

22. Pursuant to United States law, exporters and shippers or freight forwarders are required to file certain forms and declarations concerning exports of goods and technology from the United States. Typically, those filings are completed through the submission of Shipper's Export Declarations ("SED") or the submission of Electronic Export Information ("EEI") via the Automated Export Systems ("AES"). AES is administered by the U.S. Department of Homeland Security, U.S. Customs and Border Protection. The SED and EEI are official documents submitted to the United States government in connection with goods exported from the United States.

23. An essential and material part of the SED and EEI is information concerning the ultimate consignee and the country of ultimate destination of the export. In many cases, the identity of the ultimate consignee determines whether the goods may be exported a) without any specific authorization from the United States government; b) with the specific authorization or a validated license from the Department of Commerce, the Department of State, or the Department of Treasury; or c) whether the goods may not be exported from the United States.

24. Based on my training and experience, persons engaged in the illicit export or diversion of goods of United States origin to Iran often use intermediate countries to mask the true destination of the goods. These individuals take steps to conceal from the United States government, its agencies, and others, various facts regarding, among other things, the ultimate end destination. As a part of their efforts at concealment, individuals may cause other innocent parties to submit SED's or EEI's containing false information.

25. Based on my review of export documentation obtained during the course of the investigation, I was able to determine that the fifteen thermal cyclers at issue were manufactured

by Thermo Fisher, a U.S. company. Based on information provided by Thermo Fisher, the thermal cyclers were sent from their facility in Grand Island, New York on or about September 17, 2019, to the domestic purchaser, Advanced Engineering of Oconomowoc, WI.

26. On or about October 3, 2019, based on information provided by Dey Airfreight Inc., the thermal cyclers were retrieved from Advanced Engineering in Oconomowoc, Wisconsin, and transported to O'Hare International Airport, Chicago, Illinois. The thermal cyclers then were loaded on an aircraft, with the assigned airway bill number 724-3026 3155, for transport to BARAT. On that same day, Dey Airfreight Inc. filed EEI in connection with the export of the thermal cyclers. The filing listed Advanced Engineering as the United States Principal Party, Dey Airfreight Inc. as the Forwarding Agent, BARAT as the Ultimate Consignee, and United Arab Emirates as the country of ultimate destination, which, as detailed herein, is inaccurate. Niaz Ahmed was listed as the point of contact for BARAT.

Department of Commerce Post-Shipment Verifications

27. On or about January 5, 2020, a Department of Commerce Export Control Officer ("ECO") met with Akbarnia regarding six United States exports destined to BARAT and INNO TECH FZE (hereinafter, "INNO TECH"). Included in the six exports was the fifteen thermal cyclers valued at \$37,440, exported by Advanced Engineering in Oconomowoc, WI, on or about October 4, 2019 to BARAT.

28. Akbarnia told the ECO that BARAT was formerly known as INNO TECH and the company specializes in trading laboratory, medical and pharmaceutical equipment. The ECO asked if he exported to Syrian, Iran, North Korea, Sudan, Cuba, or Crimea and Akbarnia claimed he did not export to any of those countries and he only supplied UAE companies. Additionally, he claimed UAE banks would close accounts of businesses that sold to Iran. Lastly, Akbarnia

informed the ECO that he could be contacted at telephone number +971 50 108-4569 and bahador.akbarnia@gmail.com.

29. When asked about the shipments from Advanced Engineering, including the thermal cyclers shipment, Akbarnia stated that since these are older shipments, he would need some time to search his records. The ECO pointed out that the shipments were less than one year old, and several were over \$200,000 each and it seemed unusual to not know the name of his customer for these orders. Akbarnia said that he believed the shipments went to Avrasya Trading in Dubai and Flux Smooth FZE in Sharjah, or in the case of a shipment of Thermo Ion proton DNA Sequencer, that the shipment was located in storage. The ECO was told they would be able to view the stored goods at a later time and the documents for the five other shipments would be provided later.

30. Akbarnia never did provide the ECO with access to the items he claimed to have in storage, but he did provide two invoices at a later date. Neither invoice was for the thermal cyclers. On one of the invoices, only a company name was provided, and attempts by the ECO to find an address were unsuccessful. The second invoice was for a shipment of AKTA pure 150 machines and accessories going to Avrasya Trading. The ECO contacted the owner of Avrasya Trading several times attempting to get documents related to the shipment. The owner of Avrasya Trading said he had no documents and after reviewing the invoice Akbarnia provided to the ECO, the owner stated he was not certain if he ever handled the shipment. Akbarnia never provided access to the goods he claimed to have in storage and subsequent calls and emails to Akbarnia from the ECO were unanswered.

31. On or about September 18, 2014, a Department of Commerce ECO met with Akbarnia at INNO TECH, located at Block #R3-34A, SAIF Zone, Sharjah, UAE. Akbarnia's

contact information was documented as +971-50-7083299 and bahador.akbarnia@gmail.com. The purpose of the meeting was for the U.S. Department of Commerce to verify the location and/or disposition of four exports from the United States of chloroform, laboratory supplies and controlling instruments, in order to ensure that no export laws had been violated and ultimately determine if INNO TECH was a reliable recipient of U.S. goods and technology. The ECO can accomplish verification either by physically viewing and confirming the commodity on-site or, as often is the case, reviewing sales invoices and shipping documentation to establish the bona fides of the end-user.

32. The ECO explained to Akbarnia the purpose of the visit and the Post-Shipment Verification process. Akbarnia agreed to cooperate and provided that INNO TECH specializes in the acquisition and re-export of material and equipment. Akbarnia stated he was the owner and director of INNO TECH, which was established by his wife in 2012. INNO TECH employed one other person, Niaz Ahmad, who could be contacted at +971-50-7083299 and niaz231146@yahoo.com. When questioned about the four exports of chloroform, laboratory supplies and controlling equipment, Akbarnia stated that they were sent to a laboratory in Oman and provided no additional information. Akbarnia also stated that INNO TECH does not do business with Iran or Syria. The ECO made multiple requests for additional information regarding the end-use and/or end-user documentation to Akbarnia; however, no further information was provided.

OFAC License History and Determination

33. I and other law enforcement agents have checked with OFAC, the organization tasked with issuing licenses pursuant to the ECRA and IEEPA. The checks revealed that

Alwashah, Akbarnia, Moatazedi, Ahmed, Advanced Engineering, BARAT, INNO TECH, nor AHD applied for or were granted a license by OFAC.

34. Additionally, OFAC provided thermal cyclers were laboratory equipment commonly used in Polymerase Chain Reaction (PCR) machines. According to 31 C.F.R. part 560.530(a)(3), exportation and re-exportation of medicine and medical supplies to Iran requires specific authorization.

Subscribers of Google Accounts

35. Subscriber information for bahador.akbarnia@gmail.com indicated Bahador Akbarnia was the name provided for this account. The account was created on December 25, 2008, at IP address 94.101.133.202. An internet search at Ipgeolocation identified this as an Iran based IP address. This account was logged into hundreds of times between October 1, 2019 and March 2, 2020, including multiple logins from IP addresses in Iran, according to Ipgeolocation.

36. Subscriber information for mahsa.aliizadeh@gmail.com indicated Mahsa Aliizadeh was the name provided for this account. Phone number +989379003756 was associated with the account and according to a search of Country Calling Codes, the phone number was identified as Iranian. The account was created on June 6, 2014, at IP address 72.46.134.26. An internet search at Ipgeolocation identified this as a Las Vegas, Nevada, based IP address. This account had 5 successful logins between November 4, 2019 and February 13, 2020. According to Ipgeolocation, three of these logins were from IP addresses in Iran, one from the United States and one from London, England.

Contents of Akbarnia's Google Account

37. On May 6, 2020, U.S. Magistrate Judge William E. Duffin, in the Eastern District of Wisconsin, issued a search warrant for bahador.akbarnia@gmail.com and

mahsa.aliizadeh@gmail.com. Google provided account data on May 19, 2020 and analysis of account data was initiated by investigators.⁴ The bahador.akbarnia@gmail.com account contained significant communication, digital files of identification documents, business certificates and registrations; all of which are evidence of Akbarnia's scheme to acquire merchandise from the United States and re-export to end-users in Iran.

38. Akbarnia's identity documents located in the account included an Iran passport, two UK passports, Islamic Republic of Iran national card, UAE residence permit, UAE resident card, UK driver's license, and insurance card. These documents provided personal identifying information for Akbarnia such as his name, date of birth of 09/21/1976, birthplace of Roodsar, Iran, and photographs. An Islamic Republic of Iran national card for a female with last name Motazedi was also located in the account.

39. A resume for Akbarnia provided his education and employment history. In January 2001 he graduated from Gilan University⁵ after studying engineering. From March 2001 to June 2010, he held positions of sales engineer, sales manager, and member of the board for Jam Arya FanAvar⁶ in Tehran, Iran. In 2019, Akbarnia requested Dun and Bradstreet remove his and Moatazedi's name from being affiliated with Jam Arya FanAvar, claiming it was giving him problems. In 2010, Akbarnia moved to London and became a consultant and commercial advisor

⁴ A "taint review" was determined to be appropriate after attorney-client communication was located in the bahador.akbarnia@gmail.com account. This process significantly delayed the analysis of accounts subject to the warrant and collection of evidence.

⁵ The University of Guilan is an institute of higher education and graduate studies in Rasht, a large city in the province of Guilan, Iran.

⁶ Jam Aria Fan-Avar Co, Ltd of Iran appears to have been organized in 2001 as a manufacturer of life science, clinical diagnostic, and laboratory equipment and adopted the business name in 2004 after intensifying Iran sanctions.

for a company in the field of medical and laboratory products. In 2014, he became a commercial advisor for marketing and purchasing of raw materials and instruments for AHD of Tehran, Iran.

40. License Certificate 13301 from the Government of Sharjah indicated PHARMALAB FZE (hereinafter, “PHARMALAB”) was owned by Akbarnia and managed by Syed Niaz Ahmed. The original date of the certificate was 07/12/2014. The certificate listed PHARMALAB’s activities as import, export, trading of medicines, pharmaceuticals, laboratory equipment, medical equipment, and chemicals. A letter of commitment, dated March 1, 2015, was written to the Islamic Republic of Iran, Ministry of Health, Treatment and Medical Education, Medical Equipment Department, and was signed in closing by Seyed Niaz Ahmed, General Manager, PHARMALAB.

41. A tenancy contract was made in Sharjah, UAE indicating BARAT would lease P8-03-64 in the SAIF Zone for a term of one year., commencing from 06/09/2018. A Government of Sharjah Application for Change of Company Name was completed for INNO TECH, requesting proposed new names of BARAT FZE or Beacons FZE, and was signed by Shomiseh Moatazedi. The address listed was P8-03-64 and referenced license 13882.

42. Akbarnia has affiliation to SHOOKAZIST, a business in Tehran, Iran. An October 31, 2014 email from a Lebanon business to Akbarnia informed that GE requested more information regarding an OFAC license. The business included details for SHOOKAZIST and included a Microsoft PowerPoint attachment for GE’s U.S. International Trade Controls Toolkit. An April 1, 2015 email from a Netherlands business to bahador@shookazist.com and bahador.akbarnia@gmail.com, addressed to Bahador, asked if items sent arrived safe in Iran.

43. On March 14, 2019, Advanced Engineering exported CHO HCP Elisa Kit (50), protein A Mix-N-Go Elisa Kit (6), and E. Coli HCP Elisa Kit (8), purchase order 18-144 valued at

\$45,992.00, to BARAT FZE via air waybill 72430263096. An email from NIAZ1642711@GMAIL.COM on March 19, 2019, addressed to Bahador indicated the same air waybill arrived on March 17, 2019. Akbarnia responded to keep it refrigerated at customs. An email from sara.gerami@pharmalabfze.com to Akbarnia and NIAZ1642711@GMAIL.COM, dated March 19, 2019, indicated the same air waybill should be shipped as perishable by air to Tehran with the attached arrival and export documents. The email further states the description of goods should be lab supplies, the shipper should be BARAT FZE, and the receiver is CINNAGEN CO. A commercial invoice, 1903 dated 19-03-2019, located in Akbarnia's email provided the same merchandise was being sold to CINNAGEN CO, No 2, 7th ST. Simaye Iran St., Sharhrak Gharb, Tehran, Iran, phone +982142915000. Further, the invoice indicated the origin was Sweden and the total value was \$50,558.00.

44. On July 19, 2018, Advanced Engineering exported various merchandise generally described as lab equipment (including an AKTA Flux 6), purchase order 18-125 valued at \$47,661.00, to HOLDPARK LIMITED, City House, 6 Kariaskakis, Limassol, Cyprus via air waybill 11573281375. On July 26, 2018, Akbarnia emailed Cyelmar Shipping and Trading Co LTD and provided a shipment arrived at Cyprus and an export license was obtained the prior year for the same item. Akbarnia further states to remove all labels and the destination is IKA Tehran Iran. Attachments to the email included the Dey Airfreight pre alert notice to Advanced Engineering, a packing list, and commercial invoice. The packing list and commercial invoice, dated 26/07/2018 and reference 169, list the customer as SHOOKAZIST CO, No. 11, 10th Str., Mahestan Street, Shahrak Gharb, Tehran, Iran and include the same merchandise that was exported by Advanced Engineering.

45. On October 15, 2017, Akbarnia sent an email to ali.motazedi@shookazist.com with attachments concerning a co2 incubator, which included a packing list, a commercial invoice, and shipping document. The commercial invoice and packing list, reference 133 and dated 14/10/2017, provided a customer of ARYOGEN PHARMED CO, No 140, Cross Tajbakhsh Street, 24th Kilometer Makhsoos Road, Alborz, Iran and merchandise weight of 450kg. Further, the documents indicated an origin of USA. The shipping document was air waybill 17633382064 and indicated lab equipment (450kg) was sent from HOLDPARK to ARYOGEN PHARMED CO.

46. On September 27, 2017, Sheldon Manufacturing of Cornelius, Oregon, exported laboratory equipment (450kg), air waybill 12545573640, to HOLDPARK LTD. Communication for this merchandise order was initiated from HOLDPARKCY@GMAIL.COM.

47. On August 20, 2016 an email from sara.gerami@pharmalabfze.com to NIAZ1642711@GMAIL.COM and carbon copied Akbarnia, provided attachments that included a bill of lading, commercial invoice and certificate of origin. The documents indicated Advanced Engineering exported 593kg of sodium hydroxide, purchase order 16-150, to Pharmalab FZE, Office No E-84G-11, POB No 52791, Sharjah, UAE by sea freight on May 8, 2016. The email contained previous replies, which provided the shipment should arrive at the Port of Dubai on August 30, 2016, and upon arrival, it should be re-exported by sea to Bandar Abbas then to Shahriar customs in Tehran, Iran.

48. On September 21, 2017, Dr. Amir Javidtash, Commercial Manager of Arena Lifescience, Inc. sent an email to sara.gerami@pharmalabfze.com and carbon copied NIAZ1642711@GMAIL.COM and Akbarnia with instructions that exports to Iran should have labels removed, values should not be listed, and invoices should be sent with goods. Dr. Javidtash's phone number is provided in his email signature, which has international country code +98 (Iran).

49. On May 17, 2018, an email from MAHSA.ALIZADEH.83@GMAIL.COM to NIAZ1642711@GMAIL.COM and carbon copied to Akbarnia provided attachments required for a shipment to Iran. The email narrative instructed that an attached dummy invoice is just for export to Iran and should not be attached to the shipping documents because the cargo has two invoices and related packing lists, which are on INNO TECH letterhead. The packing lists indicate the merchandise was Rivaroxaban DCG, which was manufactured by LGM Pharma (USA), was contained in 12 total drums. A material safety data sheet from LGM Pharma of Nashville, TN was addressed to INNO TECH. The attached proforma invoices and packing lists, dated 02/20/2018, provided Rivaroxaban DCG were for customer ARENA HAYAT DANESH CO, No 17, 2nd Golestan Street, 3rd Boustan Street, Velenjak, Tehran, Iran.

Use of Email in International Trade and Illicit Transshipment

50. Based upon this information, as well as my training, experience, and the investigation conducted to date, I believe that there is probable cause to believe that the **Target Accounts** contain evidence, fruits, and instrumentalities of violations, attempted violations, a conspiracy to violate, and aiding and abetting and willfully causing others to violate ECRA and IEEPA. Further, because the Targets have provided e-mail accounts as a means of contact on official government forms used to facilitate the re-export of goods to Iran and have provided email accounts to U.S. officials in their official duties related to end-use checks of items sold to the Target, I believe there is probable cause that e-mail messages and other documents stored in the **Target Accounts** are likely to contain evidence of the true destination of the equipment that the Targets, using the Target Companies, ordered and evidence of intent by the Targets to evade the United States' embargo against Iran, in violation of ECRA and IEEPA.

51. Target Account 1 and Target Account 2 may also contain evidence that Alwashah had knowledge that the thermal cyclers that Advanced Engineering sent from the United States to Target Company 1 in the UAE were intended for Target Company 2 in Iran.

52. Because the Targets, using the Target Companies, appear to have evaded the United States embargo on Iran as a part of their business model, there is reason to believe that any e-mail accounts utilized by the Targets (including, but not limited to, the specific **Target Accounts** identified in the foregoing paragraphs) could contain evidence of a conspiracy to export goods of United States origin to Iran, including communications about the ultimate destination of the goods and knowledge of the embargo. Moreover, company documents (such as invoices to its customers, shipping records, and other documentation) stored by the Targets in the **Target Accounts** are likely to contain such evidence. For this reason, I respectfully submit that there is probable cause to believe the **Target Accounts** contain e-mail messages, attachments, and other documents that are evidence of federal crimes related to ECRA and IEEPA.

53. Also based on my experience, and my conversations with other law enforcement law enforcement officers, I am familiar with the practices and methods by which persons involved in criminal activity often use the Internet and electronic mail in furtherance of a variety of offenses, including those implicating national security. In particular, I am familiar with the means by which individuals often use the Internet and electronic mail to communicate electronically with others in the course of planning, executing, and concealing criminal activities, including violations of ECRA and IEEPA. I also know, based on my training and both professional and person experience, that individuals typically utilize e-mail accounts as repositories in which to store previous communications and information and continue to utilize the accounts for electronic storage for an indeterminate number of years following the conclusion of the transaction. Based on this, and the

facts set forth above, I believe there is probable cause to believe that the **Target Accounts** are likely to contain:

- a. Stored electronic mail, including unopened, read, sent, and deleted electronic mail, and all other stored electronic communications presently contained in, or on behalf of, the **Target Accounts**;
- b. Electronic mail addresses and other information stored on the contract lists associated with the **Target Accounts**;
- c. Transactional information of all activity of the electronic mail addresses and /or individual accounts described above in subparagraph (a), including log files, dates, times, methods of connecting, ports, dialups, and/or locations, including all temporarily assigned IP addresses;
- d. Logs of all access to the accounts described above, including but not limited to all electronic mail messages sent from the accounts, including dates and times of access and the Internet Protocol addresses from which the accounts were accessed;
- e. Subscriber information, in any form kept, pertaining to the electronic mail addresses and/or individual accounts described above in subparagraph (a), including applications, subscribers' full names, all screen names associated with the subscribers and/or accounts, all account names associated with the subscribers, methods of payment, telephone numbers, addresses, and detailed billing records; and
- f. Records indicating the service available to subscribers of the electronic mail addresses and/or individual accounts described above in subparagraph (a).

BACKGROUND CONCERNING EMAIL

54. In general, an email that is sent to a Google LLC subscriber is stored in the subscriber's "mailbox" on Google LLC servers until the subscriber deletes the email. If the subscriber does not delete the message, the message can remain on Google LLC servers indefinitely. Even if the subscriber deletes the email, it may continue to be available on Google LLC's servers for a certain period of time.

55. In my training and experience, I have learned that Google LLC provides a variety of on-line services, including electronic mail ("email") access, to the public Google LLC allows subscribers to obtain email accounts at the domain name gmail.com, like the email accounts listed in Attachment A. Subscribers obtain an account by registering with Google LLC.

56. During the registration process, Google LLC asks subscribers to provide basic personal information. Therefore, the computers of Google LLC are likely to contain stored electronic communications (including retrieved and unretrieved email for Google LLC subscribers) and information concerning subscribers and their use of Google LLC services, such as account access information, email transaction information, and account application information. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

57. In my training and experience, email providers generally ask their subscribers to provide certain personal identifying information when registering for an email account. Such information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to

identify the account's user or users. Based on my training and my experience, I know that, even if subscribers insert false information to conceal their identity, this information often provides clues to their identity, location, or illicit activities.

58. In my training and experience, email providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (*i.e.*, session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, email providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the email account.

59. In my training and experience, in some cases, email account users will communicate directly with an email service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Email providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

60. As explained herein, information stored in connection with an email account may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, the information stored in connection with an email account can indicate who has used or controlled the account. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, email communications, contacts list, and images sent (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the account at a relevant time. Further, information maintained by the email provider can show how and when the account was accessed or used. For example, as described below, email providers typically log the Internet Protocol (IP) addresses from which users access the email account, along with the time and date of that access. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the email account access and use relating to the crime under investigation. This geographic and timeline information may tend to either inculcate or exculpate the account owner. Additionally, information stored at the user’s account may further indicate the geographic location of the account user at a particular time (*e.g.*, location information integrated into an image or video sent via email). Last, stored electronic data may provide relevant insight into the email account owner’s state of mind as it relates to the offense under investigation. For example, information in the email account may indicate the owner’s motive and intent to commit a crime (*e.g.*, communications relating to the crime), or consciousness of guilt (*e.g.*, deleting communications in an effort to conceal them from law enforcement).

CONCLUSION

61. Based on the forgoing, I request that the Court issue the proposed search warrant.

62. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. The government will execute this warrant by serving the warrant on Google LLC. Because the warrant will be served on Google LLC, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with NIAZ1642711@GMAIL.COM, HOLDPARKCY@GMAIL.COM, AND MAHSA.ALIZADEH.83@GMAIL.COM that is stored at premises owned, maintained, controlled, or operated by Google LLC, a company headquartered at Mountain View, CA.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Google LLC (the “Provider”)

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, regardless of whether such information is located within or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to the Provider, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f) on February 7, 2020 the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A:

a. The contents of all emails associated with the accounts from **June 1, 2014 to the present** including stored or preserved copies of emails sent to and from the accounts, draft emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email;

b. All records or other information regarding the identification of the accounts, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

c. The types of service utilized;

d. All records or other information stored by an individual using the accounts, including address books, contact and buddy lists, calendar data, pictures, and files; and

e. All records pertaining to communications between the Provider and any person(s) regarding the accounts, including contacts with support services and records of actions taken.

The Provider is hereby ordered to disclose the above information to the government **14 DAYS** of issuance of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, contraband, evidence, and instrumentalities of violations of 50 U.S.C. § 4819, and 50 U.S.C. § 1705, those violations involving Bahador Akbarnia, and others and occurring after **June 1, 2014**, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

- (a) Evidence of violations of the U.S. Export Control Reform Act and/or the International Emergency Powers Act;
- (b) Evidence of violations of Iranian Transactions and Sanctions Regulations;
- (c) Evidence of a conspiracy to ship items from the United States to Iran via the UAE in violation of U.S. sanctions against Iran;
- (d) Evidence indicating how and when the email accounts were accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the email accounts owners;
- (e) Evidence indicating the email accounts owners' state of mind as it relates to the crime under investigation;
- (f) The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s).
- (g) The identity of the person(s) who communicated with the user ID about matters relating to the illegal export of items to Iran, including records that help reveal their whereabouts.

**CERTIFICATE OF AUTHENTICITY OF DOMESTIC
RECORDS PURSUANT TO FEDERAL RULES OF
EVIDENCE 902(11) AND 902(13)**

I, _____, attest, under penalties of perjury by the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this certification is true and correct. I am employed by Google LLC, and my title is _____.

I am qualified to authenticate the records attached hereto because I am familiar with how the records were created, managed, stored, and retrieved. I state that the records attached hereto are true duplicates of the original records in the custody of Google, LLC. The attached records consist of _____ **[GENERALLY DESCRIBE RECORDS (pages/CDs/megabytes)]**. I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth by, or from information transmitted by, a person with knowledge of those matters, they were kept in the ordinary course of the regularly conducted business activity of Google LLC, and they were made by Google LLC as a regular practice; and

b. such records were generated by Google LLC's electronic process or system that produces an accurate result, to wit:

1. the records were copied from electronic device(s), storage medium(s), or file(s) in the custody of Google LLC in a manner to ensure that they are true duplicates of the original records; and

2. the process or system is regularly verified by Google LLC, and at all times pertinent to the records certified here the process and system functioned properly and normally.

I further state that this certification is intended to satisfy Rules 902(11) and 902(13) of the Federal Rules of Evidence.

Date

Signature